Title (en)

THREE-WAY HANDSHAKE PROTOCOL METHOD

Title (de)

DREIWEGE-HANDSHAKE-PROTOKOLLVERFAHREN

Title (fr)

PROCÉDÉ POUR UN PROTOCOLE D ÉTABLISSEMENT D UNE CONNEXION EN TROIS ÉTAPES

Publication

EP 2375627 A4 20130703 (EN)

Application

EP 09831463 A 20091208

Priority

- CN 2009075381 W 20091208
- CN 200810184137 A 20081209

Abstract (en)

[origin: EP2375627A1] A three-way handshake protocol method. The method comprises following steps: 1) an initiator sends message I to a responder; 2) the responder sends message 2 to the initiator after receiving message 1; 3) the initiator sends message 3 to the responder after receiving message 2; 4) the responder sends message 4 to the initiator after receiving message 3; 5) after the initiator receives message 4, the initiator and the responder respectively acquires corresponding Pair Temporal Key (PTK) and Key Confirmation Key (KCK). In the present invention, the initiator directly sends message 1 constructed by using a random number (I-Nonce) produced and stored in the last PTK negotiation process to the responder during updating PTK without encrypting the messages interacted in the three-way handshake, thereby the three-way handshake protocol not only has anti-replay function compared with three-step handshake of ECMA 386, but also provides better efficiency when resource is limited.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/32** (2006.01); **H04W 12/04** (2009.01); **H04W 12/06** (2009.01); **H04W 12/10** (2009.01)

CPC (source: EP)

H04L 9/0841 (2013.01); **H04L 9/0869** (2013.01); **H04L 9/0891** (2013.01); **H04L 9/3242** (2013.01); **H04L 9/3273** (2013.01); H04L 2209/80 (2013.01)

Citation (search report)

- [XI] WO 2008112455 A2 20080918 - MOTOROLA INC [US], et al
- [A] JING LIU ET AL: "Security Verification of 802.11i 4-Way Handshake Protocol", IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS, 2008 : ICC '08 ; 19 - 23 MAY 2008, BEIJING, CHINA, IEEE, PISCATAWAY, NJ, USA, 19 May 2008 (2008-05-19), pages 1642 - 1647, XP031265638, ISBN: 978-1-4244-2075-9
- [A] ANONYMOUS ED - ANONYMOUS: "International Standard - Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications AMENDMENT 6: Medium Access Control (MAC) Se", 23 July 2004, IEEE STANDARD; [IEEE STANDARD], IEEE, PISCATAWAY, NJ, USA, PAGE(S) C1 - 178, ISBN: 978-0-7381-4073-5, XP017601578
- See references of WO 2010066186A1

Cited by

WO2014091336A1; TWI566616B

Designated contracting state (EPC)

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO SE SI SK SM TR

DOCDB simple family (publication)

EP 2375627 A1 20111012; **EP 2375627 A4 20130703**; **EP 2375627 B1 20160302**; CN 101431519 A 20090513; CN 101431519 B 20110601; JP 2012511289 A 20120517; JP 5313360 B2 20131009; WO 2010066186 A1 20100617

DOCDB simple family (application)

EP 09831463 A 20091208; CN 200810184137 A 20081209; CN 2009075381 W 20091208; JP 2011539880 A 20091208